Guidance on data protection impact assessment for the telecommunications sector in Belgium

Haesaert, Ilse; van Gremberghe, Thomas; Leonard, Jan; Verbustel, Veerle; Vissers, Robin ; Skonieczka, Maciej; De Maesschalck, Elisabeth; De Wolf, Filip; Kloza, Dariusz; Casiraghi, Simone; Ioannidis, Nikolaos; Konstantinou, Ioulia; Roda, Sara; Van Dijk, Niels

Publication date:
2020

Document Version:
Final published version

Guidance
on data protection impact assessment for the telecommunications sector in Belgium

prepared by **Agoria** in consultation with **VUB–LSTS–d.pia.lab**

.AGORIA

VUB BRUSSELS LABORATORY FOR DATA PROTECTION & PRIVACY IMPACT ASSESSMENTS

Brussels – October 2020

.AGORIA

BRUSSELS LABORATORY FOR DATA PROTECTION & PRIVACY IMPACT ASSESSMENTS

version 7.0. final
30 October 2020 14:30

Agoria VZW

Bd A. Reyers 80
1030 Bruxelles
www.agoria.be

d.pia.lab

Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)
Research Group on Law, Science, Technology & Society (LSTS)
Department Metajuridica (JURI)
Faculty of Law and Criminology (RC)
Vrije Universiteit Brussel (VUB)

Pleinlaan 2
1050 Elsene, Brussels
www.dpialab.org

Editors

Ilse HAESAERT (Agoria)
Thomas VAN GREMBERGHE (Agoria)

Contributors

Telecom Operators Experts

Jan LEONARD (Orange Belgium)
Veerle VERBUSTEL (Proximus)
Robin VISSERS (Proximus)
Maciej SKONIECZKA (Proximus)
Elisabeth DE MAESSCHALCK (Telenet)
Filip DE WOLF (VOO)

VUB–LSTS–d.pia.lab External Expert Team

Dr. Dariusz KLOZA (leader)
Simone CASIRAGHI, M.Sc.
Nikolaos IOANNIDIS, LL.M. *(March 2020–October 2020)*
Ioulia KONSTANTINOU, LL.M.
Sara RODA, LL.M. *(September 2018–March 2020)*
Prof. Dr. Niels VAN DIJK (supervisor)

Contents

List of abbreviations **6**

Foreword **7**

Executive summary **9**

1 Introduction **11**

1.1 The General Data Protection Regulation and the process of Data Protection Impact Assessment *11*

1.2 Categories of personal data processed in the telecommunications sector *12*

1.3 What is the scope of this guidance? *14*

1.3.1 The right to personal data protection 14

1.3.2 The right to privacy 15

1.3.3 Other fundamental rights 17

1.4 Who can use this guidance? *17*

1.5 How to use this document? *18*

1.6 Glossary *19*

2 Background information on the concept of impact assessment **22**

2.1 The concept of a data protection impact assessment *22*

2.2 The framework for impact assessment *22*

2.3 The method for data protection impact assessment *23*

3 The process of data protection impact assessment **25**

3.1 Phase 1: Preparation of the assessment process *25*

3.1.1 Building Block 1: Preliminary description of the processing operations 25

3.1.2 Building Block 2: Screening (threshold analysis) 25

3.1.2.1 Overview 25

3.1.2.2 Data protection impact assessment for new processing operations 26

a) Processing operations requiring a DPIA 26

b) Legally binding list of the Belgian DPA 26

c) Non-binding guidelines of the European Data Protection Board 27

d) Processing operations not requiring a DPIA 28

i) Negative criteria interpreted from Article 35 GDPR 28

ii) Legally binding list of the Belgian DPA 28

3.1.2.3 Data protection impact assessment for existing operations 29

3.1.2.4 Conclusion 29

3.1.3 Building Block 3: Scoping 30

3.1.3.1 Reference criteria 30

a) In general 30

b) European personal data protection laws 30

c) National laws and decrees that are relevant for data processing operations in the telecom sector 31

d) Case law 33

e) Technical norms and standards 33

3.1.3.2 Stakeholders 34

a) Data subjects and/or their representatives 34

b) Data Protection Authority 34

3.1.3.3 Appraisal techniques and other evaluation techniques 34

3.1.4 Building Block 4: Planning of resources and preparation 34
3.1.4.1 Team of assessors 34
3.1.4.2 Knowledge 35
3.1.4.3 Resources 35
3.1.4.4 Timeline 36
3.1.4.5 Budget 36
3.1.4.6 Specific objectives of the process 36
3.1.4.7 Acceptability criteria of negative impacts 36
3.1.4.8 Stakeholders, continuity, revision 36

3.2 Phase 2: Assessment 37
3.2.1 Building Block 5: Description of the processing operations (risk context) 37
3.2.1.1 Scope 37
3.2.1.2 Contextual description 37
3.2.1.3 Technical description 37
a) Categorization of personal data 38
b) Records of processing activities 38
c) Data flows 39
d) Data transfers outside of the European Economic Area 39
3.2.2 Building Block 6: Assessment of the necessity and proportionality of the processing operations . 39
3.2.2.1 Introduction 39
3.2.2.2 Assessment of the necessity 40
a) Step 1: Identification of fundamental rights and freedoms limited by the data processing 41
b) Step 2: Definition of the objectives of the processing purpose 41
c) Step 3: Choice of the option that is effective and least intrusive 42
3.2.2.3 Assessment of the proportionality 42
a) Step 1: Assessment of the importance of the objective and whether the processing operation meets the objective 43
b) Step 2: Assessment of the scope, the extent and the intensity of the interference 43
c) Step 3: Fair balance and evaluation of the processing operation 44
d) Step 4: Identification and introduction of safeguards if the processing operation is not proportionate 44
3.2.2.4 Synthesis of recommendations concerning necessity and proportionality assessment 45
3.2.3 Building block 7: Identification of the risks related to the processing operations 45
3.2.4 Building block 8a: Inherent risk analysis 48
3.2.5 Building block 8b: Assessment of the severity of a risk 48
3.2.6 Building block 8c: Assessment of the likelihood of a risk 48
3.2.7 Building block 8d: Risk scoring 49
3.2.8 Building block 9: Risk evaluation 50
3.2.9 Building block 10: Residual risk assessment 50
3.2.10 Building block 11: Listing of the recommendations and required actions in case of residual risks 51

3.3 Phase 3: Ex post steps 52
3.3.1 Building Block 12: Prior consultation with a DPA 52
3.3.1.1 In case of high risk after realisation of the recommendations 52
3.3.1.2 Contents of the prior consultation 52
3.3.2 Building block 13: Revisiting 52

3.4 Ongoing steps 53
3.4.1 Building Block 14: Stakeholder involvement 53
3.4.1.1 What is a stakeholder consultation? 53
3.4.1.2 Whom to consult? 53
a) In general 53
b) Internal stakeholders 54
c) External stakeholders 55
3.4.1.3 How to conduct a stakeholder consultation? 55
3.4.1.4 What if there is no stakeholder consultation? 55

3.4.2 Building Block 15: Governance 56
3.4.2.1 Quality control 56
3.4.2.2 Management and accountability 56
3.4.3 Building Block 16: Documentation 57

4 References 58

5 Annexes 60

5.1 ***Annex I:*** *Is a DPIA required?* *60*

5.2 ***Annex II:*** *Non-exhaustive list of categories of personal data* *68*

5.3 ***Annex III:*** *Description of processing operations* *71*

5.4 ***Annex IV:*** *Non-exhaustive inventory of risks to the rights and freedoms of individuals* *76*
5.4.1 Personal data protection risks 76
5.4.2 Risks related to other fundamental rights (Recital 4 GDPR) 79
5.4.3 Risks related to moral and material damages as referred to in Recital 75 GDPR 80

5.5 ***Annex V:*** *Assessment of necessity* *82*
5.5.1 Checklist to assess whether the rights of the data subjects are affected 82
5.5.2 Checklist to assess the necessity of the processing operations 83

5.6 ***Annex VI:*** *Assessment of proportionality* *85*

5.7 ***Annex VII:*** *Non-exhaustive list of risk mitigation measures* *90*

List of abbreviations

WP29	Article 29 Working Party
CFR	Charter of Fundamental Rights of the EU
CJEU	Court of Justice of the EU
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
IA	impact assessment
OJ	Official Journal of the European Union

Foreword

Telecommunications providers have a considerable customer base ranging from hundreds of thousands to millions of customers. Change initiatives are launched on a yearly basis that may have an impact on the personal data of these customers.

The telecommunications sector understands the many societal concerns regarding the personal data processing operations within the sector. This is of utmost importance and this data protection impact assessment (DPIA) guidance forms part of addressing these concerns in order to obtain, keep and maintain the trust of customers and any other stakeholder in the company when processing their personal data.

With the present guidance, the telecommunications sector intends to document how it will identify, evaluate and mitigate negative impacts related to its personal data processing operations. Furthermore, conducting a DPIA forms part of the values adhered by the telecommunications sector and its social corporate responsibility.

As telecommunications providers are faced with the common challenges, the need to draft a common guidance for carrying out a DPIA raised. Telecommunications providers have moreover received a request from the Belgian Data Protection Authority (DPA) to provide a description of the risk method they use when evaluating personal data risks in the DPIA or in case of personal data breaches. In response, the telecommunications sector in Belgium feels the need for a DPIA guidance in order to be able to abide by these requirements. This guidance seeks a common approach for the telecommunications sector by providing a *framework* and a bespoken step-by-step *method* on how to conduct a DPIA, both to be operationalized through a specific *template*.

Impact assessment, and DPIA in particular, can provide several benefits to both private and public organizations to tackle the many societal concerns, such as personal data protection, for instance by contributing to informed decision-making, enhancing public participation or balancing competing interests. At the same time, however, impact assessment has also been criticized, for example for creating an unnecessary burden to organizations, lacking specific guidance, taking place too late or for not being transparent.

Particularly for the telecommunications providers, there are many advantages of common guidance, for example:

- Ability to integrate a DPIA process in an agile business environment;
- Increase in efficiency as conducting a DPIA saves unnecessary project delays and loss of potential business opportunities;
- A harmonised and uniform approach of DPIA execution, taking into account the minimalistic provisions of the GDPR in this regard;
- Avoidance of unnecessary documentation and the maintenance thereof leading to operational overhead;
- Reduction of a possibility of misalignment with DPAs.

The present document builds on the experience and expertise of both Agoria members and VUB's d.pia.lab, whose assistance Agoria sought in preparing this guidance. It is grounded in the longstanding practice of Belgian telecommunications providers in dealing with personal data protection, which is now adjusted in order to comply with the letter of the law, namely the General Data Protection Regulation (GDPR). Nonetheless, the present document will need to be periodically revised and updated as the context changes and the experience from its use grows.

Danny GODERIS, Manager Digital & Telecom

Brussels, October 2020

Executive summary

The General Data Protection Regulation (GDPR, 2018) is the core instrument of the personal data protection law in the European Union (EU) and has substantially reformed the legislative framework compared to the former applicable law, the Data Protection Directive (DPD, 1995). One of the newly introduced requirements in the GDPR has been the obligation to conduct a data protection impact assessment (DPIA) (Article 35 GDPR). With regard to this process, it constitutes a form of impact assessment (IA) and, to a large extent, is a variation of privacy impact assessment (PIA). In general, impact assessment and similar *ex ante* evaluation techniques have proliferated so as to address largely unpredictable effects of emerging technologies, before they materialize.

The objective of this guidance document is to provide the necessary foundations for the legal requirements of the process of DPIA in the heavily-regulated telecommunications sector in Belgium. The obligation to conduct a DPIA reflects the risk-based approach to the protection of personal data and the strengthening of the principle of accountability therein (Article 5(2) GDPR). Alongside many other advantages, the actors in the telecommunications sector would multiply benefit from conducting the said process, not only because it would achieve legal compliance, but also it would demonstrate a systematization of their data processing operations. Indeed, the activity of the telecommunications sector varies from continuously handling requests regarding personalized products and services, concluding contracts with customers, to optimizing the network or monitoring its performance.

In order to navigate through the assessment process, first, the essential *framework* of IA is presented. This is part of the *architecture* of impact assessment and consists of principles and conditions governing the theory and practice thereof, e.g. independence of the assessors, the reasonable transparency therein, and their adaptive and inclusive character. The second element of the architecture is the *method*, which has accordingly been tailored-down to correspond to the reality and needs of the telecommunications sector in Belgium. The selected method includes a series of building blocks, split in four phases: preparation phase, assessment phase, post-assessment phase and ongoing phase.

During the preparation phase, a preliminary description of the envisaged data processing operations is sought, in order to determine whether or not a DPIA is required. If this is true, the assessors browse through the analysis of the threshold, determining if it is likely that the processing operations may result in a high risk to the rights and freedoms of individuals. The GDPR, the European Data Protection Board (EDPB) and the national Data Protection Authorities (DPA) have assumed their role in setting such criteria of high risk. Subsequently, during the scoping step, the applicable legislation, the stakeholders and the appraisal techniques are determined, among others. The first phase is concluded with the planning of the assessment process, including resources necessary to conduct it.

The essence of the DPIA lies within the second phase, namely the assessment phase. Here, a quite extensive description of the contextual and technical aspects of the envisaged processing operations is provided. This serves as the basis for the actual assessment through two distinct appraisal techniques, as required by the GDPR, namely: a) the necessity and proportionality assessment, aiming largely to observe the proper implementation of the personal data protection principles; and b) the assessment of the risks to the rights and freedoms of data subjects, in which possible risks are identified, analysed as to their likelihood and severity, and for which mitigation measures are recommended. To that end, a rigorous method is employed, ensuring that the assessment is made on a fact-based analysis, built on sufficient, clearly described and verifiable evidence.

Next, two milestones are provided for during the post-assessment phase. In case of high residual risk, and in absence of measures or recommendations taken by the controller to mitigate the risks after conducting a DPIA process, the step of prior consultation with the DPA is triggered, in which the latter

shall be informed and act, if necessary. Moreover, this phase includes a step dedicated to the revision of a DPIA at least when there is a change of the risk represented by processing operations.

The three phases above are ceaselessly supplemented by an ongoing, cross-cutting phase, in particular encompassing the step of stakeholder involvement, the step of quality control of the assessment process and the step of documentation. All of the three remain indispensable for achieving an excellent and trustworthy result.

Lastly, a comprehensive list of annexes concludes this guidance document. The goal of the said annexes is essentially to provide inventories of relevant information for relevant building blocks (knowledge bases) as appended to the present document.